

424 Rec'd PCT/PTO 26 MAY 2000

|   |   |   |
|---|---|---|
| FORM PTO-1390 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE   |   | ATTORNEY'S DOCKET NO.<br>PHD 99-100                                 |
| TRANSMITTAL LETTER TO THE UNITED STATES DESIGNED/ELECTED OFFICE<br>(DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371   |   | U.S. Application No. (if known, see 37 CFR 1.5)<br><b>09/555304</b> |
| INTERNATIONAL APPLICATION NO<br>PCT/EP99/07019  | INTERNATIONAL FILING DATE<br>SEPTEMBER 20, 1999 | PRIORITY DATE CLAIMED<br>SEPTEMBER 30, 1998 and August 5, 1999      |
| TITLE OF INVENTION<br>ENCODING METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS   |   |   |
| APPLICANT(S) FOR DO/EO/US<br>STEFAN PHILIPP   |   |   |
| Applicant(s) herewith submit to the United States Designated/Elected Office (DO/EO/US) the following items and other information:   |   |   |
| <p>1. <input type="checkbox"/> This is a <b>FIRST</b> submission of items concerning a filing under 35 U.S.C. 371.</p> <p>2. <input type="checkbox"/> This is a <b>SECOND</b> or <b>SUBSEQUENT</b> submission of items concerning a filing under 35 U.S.C. 371.</p> <p>3. <input checked="" type="checkbox"/> This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 38(1).</p> <p>4. <input type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.</p> <p>5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371 (c)(2))</p> <p>a. <input checked="" type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau).</p> <p>b. <input type="checkbox"/> has been transmitted by the International Bureau.</p> <p>c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US).</p> <p>6. <input type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2))</p> <p>7. <input type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))</p> <p>a. <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau).</p> <p>b. <input type="checkbox"/> have been transmitted by the International Bureau.</p> <p>c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired.</p> <p>d. <input checked="" type="checkbox"/> have not been made and will not be made.</p> <p>8. <input type="checkbox"/> A translation of the amendment to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).</p> <p>9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).</p> <p>10. <input type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).</p> <p>Items 11. to 16. Below concern document(s) or information included:</p> <p>11. <input type="checkbox"/> An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98.</p> <p>12. <input checked="" type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included.</p> <p>13. <input checked="" type="checkbox"/> A <b>FIRST</b> preliminary amendment.</p> <p><input type="checkbox"/> A <b>SECOND</b> OR <b>SUBSEQUENT</b> preliminary amendment.</p> <p>14. <input type="checkbox"/> A substitute specification.</p> <p>15. <input type="checkbox"/> A change of power of attorney and/or address letter.</p> <p>16. <input checked="" type="checkbox"/> Other items or information:<br/>Charge Authorization</p> |   |   |

RECEIVED INVENTOR'S DOCKET NUMBER EL29713191745

RECEIVED - MAY 26, 2000

THIS DOCUMENT IS THE PROPERTY OF THE  
PATENT AND TRADEMARK OFFICE. IT IS TO BE  
LOANED WITH CARE AND NOT TO BE REPRODUCED  
WITHOUT PERMISSION OF THE PATENT AND TRADEMARK  
OFFICE.

THIS DOCUMENT IS THE PROPERTY OF THE  
PATENT AND TRADEMARK OFFICE. IT IS TO BE  
LOANED WITH CARE AND NOT TO BE REPRODUCED  
WITHOUT PERMISSION OF THE PATENT AND TRADEMARK  
OFFICE.

THIS DOCUMENT IS THE PROPERTY OF THE  
PATENT AND TRADEMARK OFFICE. IT IS TO BE  
LOANED WITH CARE AND NOT TO BE REPRODUCED  
WITHOUT PERMISSION OF THE PATENT AND TRADEMARK  
OFFICE.

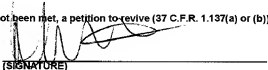
THIS DOCUMENT IS THE PROPERTY OF THE  
PATENT AND TRADEMARK OFFICE. IT IS TO BE  
LOANED WITH CARE AND NOT TO BE REPRODUCED  
WITHOUT PERMISSION OF THE PATENT AND TRADEMARK  
OFFICE.

THIS DOCUMENT IS THE PROPERTY OF THE  
PATENT AND TRADEMARK OFFICE. IT IS TO BE  
LOANED WITH CARE AND NOT TO BE REPRODUCED  
WITHOUT PERMISSION OF THE PATENT AND TRADEMARK  
OFFICE.

S:\pw\mu25pwk0.cn0

Josephine Cangelosi

Josephine Cangelosi

|  |              |  |  |
|--|--------------|--|--|
| U.S. APPLICATION NO. (If known, see 37 C.F.R. 1.5)<br><b>09/555304</b>   |              | INTERNATIONAL APPLICATION NO.<br>PCT/EP99/07019  | ATTORNEY'S DOCKET NUMBER<br>PHD 99-010 |
| 17 [ x ] The following fees are submitted:<br>BASIC NATIONAL FEE (37 C.F.R. 1.492(A)(1)-(5)):<br>Search Report has been prepared by the EPO or JPO \$940.00<br>International preliminary-examination fee paid to USPTO (37 C.F.R. 1.482) \$720.00<br>No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.448(a)(2)) \$760.00<br>Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.448(a)(2)) paid to USPTO \$970.00<br>International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) \$ 96.00<br>ENTER APPROPRIATE BASIC FEE AMOUNT = \$870.00 |              |  | CALCULATIONS (PTO USE ONLY)            |
| Surcharge of \$130.00 for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).   |              |  | \$                                     |
| CLAIMS   | NUMBER FILED | NUMBER EXTRA   | RATE                                   |
| Total Claims   | 4 - 20 =     |  | X \$ 18.00                             |
| Independent claims   | 1 - 3 =      |  | X \$ 78.00                             |
| MULTIPLE DEPENDENT CLAIMS (if applicable)  |              |  | + \$260.00                             |
| TOTAL OF ABOVE CALCULATIONS =  |              |  | \$970.00                               |
| Reductions by 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 C.F.R. 1.9, 1.27, 1.28)   |              |  | \$                                     |
| SUBTOTAL =   |              |  | \$970.00                               |
| Processing fee of \$130.00 for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 C.F.R. 1.492(f)).  |              |  | \$                                     |
| TOTAL NATIONAL FEE =   |              |  | \$                                     |
| Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). \$40.00 per property   |              |  | \$ 40.00                               |
| TOTAL FEES ENCLOSED =  |              |  | \$1,010.00                             |
|  |              |  | Amount to be Refunded \$               |
|  |              |  | Charged \$                             |
| a. [ ] A check in the amount \$ _____ to cover the above fees is enclosed.<br>b. [ X ] Please charge my Deposit Account No. <u>14-1270</u> in the amount of \$ <u>1,010.00</u> to cover the above fees. A duplicate copy of this sheet is enclosed.<br>c. [ X ] The Commissioner is hereby authorized to charge any additional fee, with the exception of the Base Issue Fee, which may be required, or credit any overpayment to Deposit Account No. <u>14-1270</u> . A duplicate copy of this sheet is enclosed.   |              |  |  |
| NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.  |              |  |  |
| SEND ALL CORRESPONDENCE TO:<br>Corporate Patent Counsel<br>Philips Electronics North America Corporation<br>580 White Plains Road<br>Tarrytown, NY 10591   |              |  |  |
| DATE OF MAILING:<br><u>5/26/00</u>   |              | (SIGNATURE)<br><br>Daniel J. Piotrowski<br>(NAME)<br>42,079<br>(REGISTRATION NUMBER) |  |

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Atty. Docket

STEFAN PHILIPP

PHD 99-100

Serial No.

Filed: Concurrently

ENCODING METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS

Honorable Commissioner of Patents and Trademarks  
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to calculation of the filing fee and examination, please amend the above-identified application as follows:

IN THE CLAIMS

Please amend claim 4 as follows:

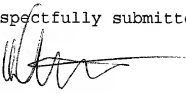
Claim 4, line 1, change "one of the preceding Claims" to  
--Claim 1--.

## REMARKS

The claims are amended to remove multiple dependency without change in scope.

Entry of the Amendment is respectfully requested.

Respectfully submitted,



By

Daniel J. Piotrowski, Reg. 42,079  
Attorney  
(914) 333-9624

1/PR+5

Encoding method for carrying out cryptographic operations.Technical field

The invention relates to an encryption method as disclosed in the introductory part of Claim 1, wherein at least one cryptographic sub-operation is performed on digital data stored as at least one data bit word in a storage cell or a register.

5 State of the art

Cryptographic operations are carried out in many data processing apparatus so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried out by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a  
10 chip card or an IC card. For such cryptographic calculations it is often necessary to initialize relevant storage sections or registers of the data processing apparatus with operands. Data or intermediate results used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

In order to calculate the cryptographic algorithms, logic combinations of  
15 operands or intermediate results are formed in the data processing apparatus. Depending on the technology used, such operations, notably the loading of empty or previously erased storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of the current consumption occurs when the value of a bit storage cell changes, i.e. when its  
20 value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the Hamming weight of the operand (= number of bits having the value "1") written into the empty register. Analysis of this current variation could thus enable  
25 extraction of information concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. When several current measurements are performed on the data processing apparatus, adequate information could be extracted, for example in the case of very small signal variations. On the other hand, a plurality of current measurements could also enable a possibly required differentiation. This

type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus.

5 EP 0 482 975 B1 discloses a memory card which includes a microcircuit and at least one memory which is connected to a data processing member, the data processing member being controlled by a data signal from outside the card and delivering a command transmission signal in response to said data signal, at a given instant, said command transmission signal being delayed by a predetermined period of time (T) relative to the  
10 reception of the data signal, the period of time (T) being selected so as to be variable in time on a random basis in order to enhance the security. Crypto analysis on the basis of a current variation during the writing of the memory, however, cannot be precluded by such a system.

#### Implementation of the invention, object, solution, advantages

15 It is an object of the present invention to provide an improved method of the kind set forth which eliminates the described drawbacks and effectively prevents crypto analysis by observation of current consumption of a data processing apparatus.

This object is achieved by means of a method of the kind set forth which is characterized as disclosed in Claim 1.

20 To this end, in conformity with the invention a data bit word generated on the basis of random numbers is stored in a storage cell before a data bit word is written therein.

This offers the advantage that there is a non-predetermined or non-predeterminable pre-initialization which prevents information concerning the data bit word written into the memory cell from being extracted on the basis of variations of the current  
25 consumption during the writing into the storage cell. During the writing of data in such pre-initialized storage cells the current consumption changes exclusively in dependence on a difference between the Hamming weight of the written data and the unknown random number, so that this difference, and hence also the variation of the current consumption, is of a random nature and cannot be determined in advance.

30 There are various possibilities for the implementation of the method. According to a preferred version, the bit word based on random numbers is written into the storage cell by a processor. Alternatively, the bit word based on random numbers is written into the storage cell via a direct connection between a random number source and the storage cell.

Temporal correlation between the writing of the random number into a storage cell and the cryptographic sub-operation is avoided in that the bit word based on random numbers is stored in the storage cell at an instant in time which precedes the cryptographic sub-operation.

#### Brief description of the drawings

The invention will be described in detail hereinafter with reference to the accompanying drawings. The single Figure thereof shows a flow chart concerning a preferred version of the method according to the invention.

#### Preferred implementation of the invention

As is shown in the sole Figure, a storage cell 10 or a register is provided for the writing and storage of data  $x_i$  in the form of a data bit word via a connection 11. However, before the operand  $x_i$  is written into the storage cell 10, a random number source 12 generates random numbers which are written or stored, via a direct connection 14, into the memory cell 10. In other words, the storage cell 10 is initialized by way of a random value  $r_i$ . Alternatively, the random value  $r_i$  can also be written, via the connection 11, by a processor having previously received the random value from the random number source 12.

The instant of pre-initialization can be selected at random and preferably does not directly precede the cryptographic operation. Preferably, repeated pre-initialization of the storage section or register is performed with varying random numbers.

When the storage sections or registers thus pre-initialized are loaded with data  $x_i$  in the course of a cryptographic operation, the current consumption will change exclusively in dependence on a difference between the Hamming weight of the operand  $x_i$  and the Hamming weight of the unknown random number. It is impossible to extract information as regards the operands used or intermediate results on the basis of such a random difference value.

## CLAIMS:

1. An encryption method wherein at least one cryptographic sub-operation is performed on digital data stored as at least one data bit word in a storage cell (10) or a register, characterized in that

5 a data bit word generated on the basis of random numbers is stored in a storage cell (10) before a data bit word is written therein.

2. An encryption method as claimed in Claim 1, characterized in that

10 the bit word based on random numbers is written into the storage cell (10) by a processor.

3. An encryption method as claimed in Claim 1, characterized in that

15 the bit word based on random numbers is written into the storage cell (10) via a direct connection between a random number source (12) and the storage cell.

4. An encryption method as claimed in one of the preceding Claims, characterized in that

the bit word based on random numbers is stored in the storage cell (10) at an instant in time which precedes the cryptographic sub-operation.

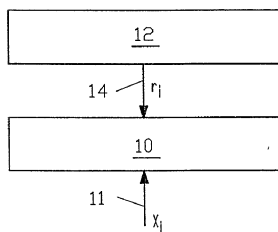


## LIST OF REFERENCES

|   |       |                       |
|---|-------|-----------------------|
|   | 10    | storage cell/register |
|   | 11    | connection            |
| 5 | 12    | random number source  |
|   | 14    | connection            |
|   | $x_i$ | data                  |
|   | $T_i$ | random value.         |

## ABSTRACT:

The invention proposes an encryption method wherein a cryptographic sub-operation is performed on digital data which are stored as at least one data bit word in a storage cell (10) or a register and wherein successful crypto analysis by observation of current consumption of a data processing apparatus is effectively prevented by writing a data  
5 bit word based on random numbers into a storage cell (10) before a data bit word is written therein.



## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Atty. Docket

STEFAN PHILIPP

PHD 99-100

Serial No.

Group Art Unit:

Filed: CONCURRENTLY

Examiner:

ENCODING METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS

Honorable Commissioner of Patents and Trademarks  
Washington, D.C. 20231APPOINTMENT OF ASSOCIATES

Sir:

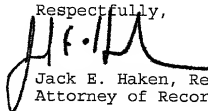
The undersigned Attorney of Record hereby revokes all prior appointments (if any) of Associate Attorney(s) or Agent(s) in the above-captioned case and appoints:

**DANIEL J. PIOTROWSKI**(Registration No. 42,079)

c/o U.S. PHILIPS CORPORATION, Intellectual Property Department, 580 White Plains Road, Tarrytown, New York 10591, his Associate Attorney(s)/Agent(s) with all the usual powers to prosecute the above-identified application and any division or continuation thereof, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

ALL CORRESPONDENCE CONCERNING THIS APPLICATION AND THE LETTERS PATENT WHEN GRANTED SHOULD BE ADDRESSED TO THE UNDERSIGNED ATTORNEY OF RECORD.

Respectfully,



Jack E. Haken, Reg. 26,902  
Attorney of Record

Dated at Tarrytown, New York  
this 24TH day of MAY, 2000  
S:FPW\MU25PWLO.CNO

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: "Encoding method for carrying out cryptographic operations"

the specification of which (check only one item below):

☐ is attached hereto.

☐ was filed as United States application

Serial No

on

and was amended

on

☒ was filed as PCT international application

Number PCT/EP99/07019

on 20 September 1999 (20.09.99)

and was amended under PCT Article 19

on (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S) AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. 119:

| COUNTRY | APPLICATION NUMBER | DATE OF FILING<br>DAY, MONTH, YEAR | PRIORITY<br>CLAIMED UNDER<br>35 USC 119 |
|---------|--------------------|------------------------------------|---|
| Germany | 19845096.6         | 30 September 1998                  | YES                                     |
| Germany | 19936890.2         | 5 August 1999                      | YES                                     |
|         |                    |                                    |   |
|         |                    |                                    |   |

**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (List name and registration number)

**Algy Tamoshunas Reg. No. 27,677**  
**Jack E. Haken, Reg. No. 26,902**

Direct Telephone Calls to:  
(name and telephone number)  
(914)332-0222

|     |                         |                     |                          |                          |
|-----|-------------------------|---------------------|--------------------------|--------------------------|
| 201 | FULL NAME OF INVENTOR   | FAMILY NAME         | FIRST GIVEN NAME         | SECONDE GIVEN NAME       |
|     | RESIDENCE & CITIZENSHIP | CITY                | STATE OR FOREIGN COUNTRY | COUNTRY OF CITIZENSHIP   |
|     | POST OFFICE ADDRESS     | POST OFFICE ADDRESS | CITY                     | STATE & ZIP CODE/COUNTRY |
| 202 | FULL NAME OF INVENTOR   | FAMILY NAME         | FIRST GIVEN NAME         | SECONDE GIVEN NAME       |
|     | RESIDENCE & CITIZENSHIP | CITY                | STATE OR FOREIGN COUNTRY | COUNTRY OF CITIZENSHIP   |
|     | POST OFFICE ADDRESS     | POST OFFICE ADDRESS | CITY                     | STATE & ZIP CODE/COUNTRY |
| 203 | FULL NAME OF INVENTOR   | FAMILY NAME         | FIRST GIVEN NAME         | SECONDE GIVEN NAME       |
|     | RESIDENCE & CITIZENSHIP | CITY                | STATE OR FOREIGN COUNTRY | COUNTRY OF CITIZENSHIP   |
|     | POST OFFICE ADDRESS     | POST OFFICE ADDRESS | CITY                     | STATE & ZIP CODE/COUNTRY |
| 204 | FULL NAME OF INVENTOR   | FAMILY NAME         | FIRST GIVEN NAME         | SECONDE GIVEN NAME       |
|     | RESIDENCE & CITIZENSHIP | CITY                | STATE OR FOREIGN COUNTRY | COUNTRY OF CITIZENSHIP   |
|     | POST OFFICE ADDRESS     | POST OFFICE ADDRESS | CITY                     | STATE & ZIP CODE/COUNTRY |
| 205 | FULL NAME OF INVENTOR   | FAMILY NAME         | FIRST GIVEN NAME         | SECONDE GIVEN NAME       |
|     | RESIDENCE & CITIZENSHIP | CITY                | STATE OR FOREIGN COUNTRY | COUNTRY OF CITIZENSHIP   |
|     | POST OFFICE ADDRESS     | POST OFFICE ADDRESS | CITY                     | STATE & ZIP CODE/COUNTRY |
| 206 | FULL NAME OF INVENTOR   | FAMILY NAME         | FIRST GIVEN NAME         | SECONDE GIVEN NAME       |
|     | RESIDENCE & CITIZENSHIP | CITY                | STATE OR FOREIGN COUNTRY | COUNTRY OF CITIZENSHIP   |
|     | POST OFFICE ADDRESS     | POST OFFICE ADDRESS | CITY                     | STATE & ZIP CODE/COUNTRY |

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 if Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

|                           |                           |                           |
|---------------------------|---------------------------|---------------------------|
| SIGNATURE OF INVENTOR 201 | SIGNATURE OF INVENTOR 202 | SIGNATURE OF INVENTOR 203 |
| DATE April 20, 2000       | DATE                      | DATE                      |
| SIGNATURE OF INVENTOR 204 | SIGNATURE OF INVENTOR 205 | SIGNATURE OF INVENTOR 206 |
| DATE                      | DATE                      | DATE                      |